



Japan Patent Office

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: January 22, 2003

Application Number: Japanese Patent Application  
No.2003-013591

[ST.10/C]: [JP2003-013591]

Applicant(s): RICOH COMPANY, LTD.

December 18, 2003

Commissioner,  
Japan Patent Office

Yasuo Imai (Seal)

Certificate No.2003-3105096

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

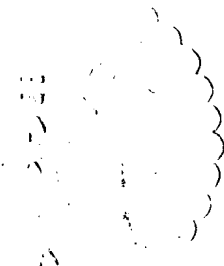
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日                      2 0 0 3 年    1 月 2 2 日  
Date of Application:

出 願 番 号                      特 願 2 0 0 3 - 0 1 3 5 9 1  
Application Number:

[ST. 10/C] :                      [ J P 2 0 0 3 - 0 1 3 5 9 1 ]

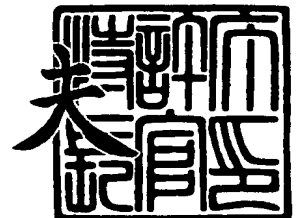
出      願                      人                      株式会社リコー  
Applicant(s):



2 0 0 3 年 1 2 月 1 8 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康



出証番号    出証特 2 0 0 3 - 3 1 0 5 0 9 6



【書類名】 特許願

【整理番号】 0206608

【提出日】 平成15年 1月22日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 H04N 1/41

【発明の名称】 画像符号化装置、符号復号化装置、プログラム及び記憶媒体

【請求項の数】 27

【発明者】

【住所又は居所】 鳥取県鳥取市千代水1丁目100番地 アイシン千代ビル リコー鳥取技術開発株式会社内

【氏名】 西村 隆之

【発明者】

【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内

【氏名】 野水 泰之

【発明者】

【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内

【氏名】 作山 宏幸

【発明者】

【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内

【氏名】 原 潤一

【発明者】

【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内

【氏名】 松浦 熱河

【発明者】

【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内

【氏名】 矢野 隆則

**【発明者】****【住所又は居所】** 東京都大田区中馬込1丁目3番6号 株式会社リコー内**【氏名】** 児玉 卓**【発明者】****【住所又は居所】** 東京都大田区中馬込1丁目3番6号 株式会社リコー内**【氏名】** 宮澤 利夫**【発明者】****【住所又は居所】** 東京都大田区中馬込1丁目3番6号 株式会社リコー内**【氏名】** 新海 康行**【特許出願人】****【識別番号】** 000006747**【氏名又は名称】** 株式会社リコー**【代表者】** 桜井 正光**【代理人】****【識別番号】** 100101177**【弁理士】****【氏名又は名称】** 柏木 慎史**【電話番号】** 03(5333)4133**【選任した代理人】****【識別番号】** 100102130**【弁理士】****【氏名又は名称】** 小山 尚人**【電話番号】** 03(5333)4133**【選任した代理人】****【識別番号】** 100072110**【弁理士】****【氏名又は名称】** 柏木 明**【電話番号】** 03(5333)4133

## 【手数料の表示】

【予納台帳番号】 063027

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9808802

【包括委任状番号】 0004335

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 画像符号化装置、符号復号化装置、プログラム及び記憶媒体

【特許請求の範囲】

【請求項 1】 入力された画像データを J P E G 2 0 0 0 アルゴリズムに従い圧縮符号化する圧縮符号化手段と、

この圧縮符号化手段により可逆圧縮符号化される直前のデータをパスワード入力に基づき解除可能にスクランブル化して可逆圧縮符号化に供するスクランブル化手段と、

を備えることを特徴とする画像符号化装置。

【請求項 2】 前記スクランブル化手段は、データのランダム化によりスクランブル化することを特徴とする請求項 1 記載の画像符号化装置。

【請求項 3】 スクランブル前のデータとスクランブルデータとの間の差分値をランダム化により復元可能に暗号化した電子透かしデータとしてスクランブル後のデータ中に埋め込む電子透かし埋め込み手段を備えることを特徴とする請求項 1 又は 2 記載の画像符号化装置。

【請求項 4】 電子透かし埋め込み手段は、ランダム化により復元可能に暗号化するための種データとしてパスワードとスクランブル前のデータとを用いることを特徴とする請求項 3 記載の画像符号化装置。

【請求項 5】 前記圧縮符号化手段は、入力された画像データを J P E G 2 0 0 0 アルゴリズムの可逆モードに従い圧縮符号化するものであり、

前記スクランブル化手段は、前記圧縮符号化手段による離散ウェーブレット変換処理前の画像データをスクランブル化する、

ことを特徴とする請求項 1 ないし 4 の何れか一記載の画像符号化装置。

【請求項 6】 前記圧縮符号化手段は、入力された画像データを J P E G 2 0 0 0 アルゴリズムの非可逆モードに従い圧縮符号化するものであり、

前記スクランブル化手段は、前記圧縮符号化手段による離散ウェーブレット変換処理後に量子化された離散ウェーブレット変換係数をスクランブル化する、

ことを特徴とする請求項 1 ないし 4 の何れか一記載の画像符号化装置。

【請求項 7】 前記スクランブル化手段は、量子化としてビットプレーン化

された離散ウェーブレット変換係数であるビット係数の有意係数を対象としてスクランブル化する、ことを特徴とする請求項6記載の画像符号化装置。

【請求項8】 前記スクランブル化手段は、スクランブル化により対象となるビット係数を反転させる場合には隣り桁のビット係数を反転させる、ことを特徴とする請求項7記載の画像符号化装置。

【請求項9】 前記スクランブル化手段は、量子化された離散ウェーブレット変換係数に対するスクランブルレベルが可変設定自在である、ことを特徴とする請求項6ないし8の何れか一記載の画像符号化装置。

【請求項10】 ビットプレーン化された離散ウェーブレット変換係数であるビット係数のビット位置の選択によりスクランブルレベルが可変設定自在である、ことを特徴とする請求項9記載の画像符号化装置。

【請求項11】 離散ウェーブレット変換係数のうちの離散ウェーブレット変換処理によるサブバンドの階層位置の選択によりスクランブルレベルが可変設定自在である、ことを特徴とする請求項9記載の画像符号化装置。

【請求項12】 離散ウェーブレット変換による符号化単位となる複数の矩形領域が集合しスクランブル化が施されるブロックの大きさの選択によりスクランブルレベルが可変設定自在である、ことを特徴とする請求項9記載の画像符号化装置。

【請求項13】 請求項1ないし12の何れか一記載の画像符号化装置によりスクランブル化された符号データの入力を受付ける符号データ入力手段と、

入力された符号データをJ P E G 2 0 0 0アルゴリズムに従い画像データに復号する復号化手段と、

パスワード入力に基づき前記復号化手段による復号処理において符号データに対するスクランブルを解除するデスクランブル化手段と、  
を備えることを特徴とする符号復号化装置。

【請求項14】 コンピュータにインストールされ、又は、解釈されて、当該コンピュータに、

入力された画像データをJ P E G 2 0 0 0アルゴリズムに従い圧縮符号化する圧縮符号化機能と、

この圧縮符号化機能により可逆圧縮符号化される直前のデータをパスワード入力に基づき解除可能にスクランブル化して可逆圧縮符号化に供するスクランブル化機能と、

を実行させる画像符号化用プログラム。

【請求項 15】 前記スクランブル化機能は、データのランダム化によりスクランブル化することを特徴とする請求項 14 記載の画像符号化用プログラム。

【請求項 16】 スクランブル前のデータとスクランブルデータとの間の差分値をランダム化により復元可能に暗号化した電子透かしデータとしてスクランブル後のデータ中に埋め込む電子透かし埋め込み機能を前記コンピュータに実行させることを特徴とする請求項 14 又は 15 記載の画像符号化用プログラム。

【請求項 17】 電子透かし埋め込み機能は、ランダム化により復元可能に暗号化するための種データとしてパスワードとスクランブル前のデータとを用いることを特徴とする請求項 16 記載の画像符号化用プログラム。

【請求項 18】 前記圧縮符号化機能は、入力された画像データを J P E G 2 0 0 0 アルゴリズムの可逆モードに従い圧縮符号化するものであり、

前記スクランブル化機能は、前記圧縮符号化手段による離散ウェーブレット変換処理前の画像データをスクランブル化する、  
ことを特徴とする請求項 13 ないし 17 の何れか一記載の画像符号化用プログラム。

【請求項 19】 前記圧縮符号化機能は、入力された画像データを J P E G 2 0 0 0 アルゴリズムの非可逆モードに従い圧縮符号化するものであり、

前記スクランブル化機能は、前記圧縮符号化手段による離散ウェーブレット変換処理後に量子化された離散ウェーブレット変換係数をスクランブル化する、  
ことを特徴とする請求項 13 ないし 17 の何れか一記載の画像符号化用プログラム。

【請求項 20】 前記スクランブル化機能は、量子化としてビットプレーン化された離散ウェーブレット変換係数であるビット係数の有意係数を対象として



スクランブル化する、ことを特徴とする請求項 19 記載の画像符号化用プログラム。

【請求項 21】 前記スクランブル化機能は、スクランブル化により対象となるビット係数を反転させる場合には隣り桁のビット係数を反転させる、ことを特徴とする請求項 20 記載の画像符号化用プログラム。

【請求項 22】 前記スクランブル化機能は、量子化された離散ウェーブレット変換係数に対するスクランブルレベルが可変設定自在である、ことを特徴とする請求項 19 ないし 21 の何れか一記載の画像符号化用プログラム。

【請求項 23】 ビットプレーン化された離散ウェーブレット変換係数であるビット係数のビット位置の選択によりスクランブルレベルが可変設定自在である、ことを特徴とする請求項 24 記載の画像符号化用プログラム。

【請求項 24】 離散ウェーブレット変換係数のうちの離散ウェーブレット変換処理によるサブバンドの階層位置の選択によりスクランブルレベルが可変設定自在である、ことを特徴とする請求項 22 記載の画像符号化用プログラム。

【請求項 25】 離散ウェーブレット変換による符号化単位となる複数の矩形領域が集合しスクランブル化が施されるブロックの大きさの選択によりスクランブルレベルが可変設定自在である、ことを特徴とする請求項 22 記載の画像符号化用プログラム。

【請求項 26】 コンピュータにインストールされ、又は、解釈されて、当該コンピュータに、

請求項 1 ないし 12 の何れか一記載の画像符号化装置によりスクランブル化された符号データの入力を受付ける符号データ入力機能と、

入力された符号データを J P E G 2 0 0 0 アルゴリズムに従い画像データに復号する復号化機能と、

パスワード入力に基づき前記復号化機能による復号処理において符号データに対するスクランブルを解除するデスクランブル化機能と、  
を実行させることを特徴とする符号復号化用プログラム。

【請求項 27】 請求項 13 ないし 26 の何れか一記載のプログラムを格納しているコンピュータ読取り可能な記憶媒体。

**【発明の詳細な説明】****【0001】****【発明の属する技術分野】**

本発明は、画像符号化装置、符号復号化装置、プログラム及び記憶媒体に関する。

**【0002】****【従来の技術】**

近年、インターネットやパソコン等の普及・発展に伴い、インターネットを通じたデジタルデータの通信が幅広く行われるようになってきている。ここに、このようなデジタルデータの送信者は、そのデータを符号化して送信するようにしている。現に、プロバイダ等のデータ送信者（配布者）は、符号化された画像データを不特定多数の利用者に送信して配給するサービスを行っている。このようなサービスの一つとして、通信販売等に置ける商品紹介に関するようなデータを、インターネットを通じて利用者に配信することが考えられる。この場合、プロバイダに対して予め料金を支払っている利用者（閲覧資格者）が、その支払った金額に応じて、受信した符号化データを復号して閲覧できるサービスである。

**【0003】**

しかしながら、このように不特定多数の人に符号化データを配信するサービスにおいては、閲覧資格者のみはその符号化されたデータを正しく復号できなければ意味がない。かといって、将来、プロバイダと契約して閲覧資格者となる可能性のある一般ユーザが、全く、その符号化された画像データを認識できないと、元々興味を引かず、その閲覧資格者数の増大を見込めない。

**【0004】**

このようなことから、この種の符号データに関しては、スクランブル処理した符号データとして配信する一方、閲覧資格者には復号時にスクランブルを解除するためのソフトウェア等を配布しておくことで、閲覧資格者は復号時にはスクランブルを解除して本来の正常な画像を閲覧できるようにするスクランブル方式が広く用いられている。このようにスクランブル処理することで、閲覧資格のないユーザは、本来の画像としては見にくかったり多少判りにくくなったりするが、

逆に、本来の画像を見たくなる等の宣伝効果が生じ、閲覧資格者数の増大を見込めることとなる。

#### 【0005】

このようなスクランブル方式に関しては、多数の提案例がある。そのうち、例えば、ラインローテーション、ラインバーミュテーション等のようにデータ列の並べ替えによって実現する方式と(例えば、特許文献1参照)、画像データのランダム化(乱数暗号化)によって実現する方式と、その他の方式(例えば、色空間軸の回転方式)等がある(これらについては、例えば、特許文献2参照)。

#### 【0006】

##### 【特許文献1】

特開 2001-218184 公報

##### 【特許文献2】

特開 2000-115581 公報

#### 【0007】

##### 【発明が解決しようとする課題】

しかし、このような従来のスクランブル方式は、程度の差はあれ、スクランブル処理に伴う画像の劣化が必然であり、かつ、その劣化の歯止めも必然となるが、これらを両立していない現状にある。

#### 【0008】

即ち、画像データにスクランブルをかけても、そのスクランブルを解除した場合には、スクランブルの影響が残ることなくスクランブル前の元の画像データの状態に復元できることが必要であるが、例えば、特許文献1の場合であれば、周波数帯域のデータを並び換えるスクランブル処理を行った後、圧縮効率を向上させるための非可逆な量子化を行ってから、エントロピー符号化を行っているため、スクランブル解除の際には非可逆処理となってしまう、元のデータに完全には戻せないため、スクランブルの影響が残ってしまう可能性がある。

#### 【0009】

また、画像データにスクランブルをかけるにしても、画像データによってはスクランブルにより画像をかなり見にくくしたい場合やあまり見にくくしたくない

場合等があるが、その程度が一律であるため、プロバイダにおいて個々の画像データに応じて適切なレベルに画質を劣化させるスクランブル画像の提供が困難な現状にある。

#### 【0010】

本発明の目的は、スクランブルの影響が残らない復号処理を可能にすることである。

#### 【0011】

加えて、本発明の目的は、スクランブルによる画質の劣化レベルを加減できるようにすることである。

#### 【0012】

##### 【課題を解決するための手段】

請求項1記載の発明の画像符号化装置は、入力された画像データをJ P E G 2 0 0 0 アルゴリズムに従い圧縮符号化する圧縮符号化手段と、この圧縮符号化手段により可逆圧縮符号化される直前のデータをパスワード入力に基づき解除可能にスクランブル化して可逆圧縮符号化に供するスクランブル化手段と、を備える。

#### 【0013】

従って、可逆圧縮符号化される直前のデータをスクランブル化した後、当該入力された画像データはJ P E G 2 0 0 0 アルゴリズムに従い圧縮符号化されるので、復号に際してもスクランブルデータまでは劣化することなく必ず可逆圧縮符号化により完全に元の状態に戻すことができ、当該スクランブルの影響が残らないスクランブル解除が可能となる。また、パスワード入力に基づき解除可能なスクランブル化であり、スクランブル解除には所定のパスワード入力を必要とし、当該画像データの閲覧許可者のみへの公開を実現できる。

#### 【0014】

請求項2記載の発明は、請求項1記載の画像符号化装置において、前記スクランブル化手段は、データのランダム化によりスクランブル化する。

#### 【0015】

従って、データ列の並べ換え方式等のような境界線の不透明の問題を伴うこと

なく、データを適正にスクランブルさせることができる。

【0016】

請求項3記載の発明は、請求項1又は2記載の画像符号化装置において、スクランブル前のデータとスクランブルデータとの間の差分値をランダム化により復元可能に暗号化した電子透かしデータとしてスクランブル後のデータ中に埋め込む電子透かし埋め込み手段を備える。

【0017】

従って、このような暗号化した電子透かしデータをスクランブル後のデータ中に埋め込むことにより、特別なソフト実行のみによりスクランブル前の元のデータの復元が可能となる。

【0018】

請求項4記載の発明は、請求項3記載の画像符号化装置において、電子透かし埋め込み手段は、ランダム化により復元可能に暗号化するための種データとしてパスワードとスクランブル前のデータとを用いる。

【0019】

従って、埋め込まれる電子透かしを第三者に解読しにくくさせることができ、スクランブル化されたデータを元に戻すための電子透かしデータの安全性が向上する。

【0020】

請求項5記載の発明は、請求項1ないし4の何れか一記載の画像符号化装置において、前記圧縮符号化手段は、入力された画像データをJ P E G 2 0 0 0アルゴリズムの可逆モードに従い圧縮符号化するものであり、前記スクランブル化手段は、前記圧縮符号化手段による離散ウェーブレット変換処理前の画像データをスクランブル化する。

【0021】

従って、入力された画像データをJ P E G 2 0 0 0アルゴリズムの可逆モードに従い圧縮符号化する場合であれば、離散ウェーブレット変換処理前の画像データであっても可逆的に完全に復号されるので、この時点の画像データにスクランブルをかけてもそのスクランブルも可逆的に完全に復号させることで、完全にス

クランブルの影響をなくすることが可能となる。

【0022】

請求項6記載の発明は、請求項1ないし4の何れか一記載の画像符号化装置において、前記圧縮符号化手段は、入力された画像データをJ P E G 2 0 0 0アルゴリズムの非可逆モードに従い圧縮符号化するものであり、前記スクランブル化手段は、前記圧縮符号化手段による離散ウェーブレット変換処理後に量子化された離散ウェーブレット変換係数をスクランブル化する。

【0023】

従って、入力された画像データをJ P E G 2 0 0 0アルゴリズムの非可逆モードに従い圧縮符号化する場合であっても、量子化処理の後は可逆的な処理となるので、その直前のデータである離散ウェーブレット変換処理後に量子化された離散ウェーブレット変換係数にスクランブルをかけてもそのスクランブルも可逆的に完全に復号させることで、完全にスクランブルの影響をなくすることが可能となる。

【0024】

請求項7記載の発明は、請求項6記載の画像符号化装置において、前記スクランブル化手段は、量子化としてビットプレーン化された離散ウェーブレット変換係数であるビット係数の有意係数を対象としてスクランブル化する。

【0025】

ここに、「ビット係数の有意係数」とは、例えばビット表現した処理対象となるビットプレーン化された離散ウェーブレット変換係数を上位ビットから下位ビット方向に符号化する場合に、注目するビット係数が0でないことが判っている係数をいう。

【0026】

従って、このようなビットプレーン化された離散ウェーブレット変換係数であるビット係数の有意係数を対象としてスクランブル化することで、効果的なスクランブルをかけることができる。

【0027】

請求項8記載の発明は、請求項7記載の画像符号化装置において、前記スクラ

ンブル化手段は、スクランブル化により対象となるビット係数を反転させる場合には隣り桁のビット係数を反転させる。

#### 【0028】

従って、スクランブル化により対象となるビット係数を反転させる場合には、そのビット係数の反転処理よりこの部分で極端に表示画像の明るさが変わってしまうことがあるが、併せて、直上桁又は直下桁なる隣り桁のビット係数を反転させることで、緩和させることができる。

#### 【0029】

請求項9記載の発明は、請求項6ないし8の何れか一記載の画像符号化装置において、前記スクランブル化手段は、量子化された離散ウェーブレット変換係数に対するスクランブルレベルが可変設定自在である。

#### 【0030】

従って、量子化された離散ウェーブレット変換係数に対するスクランブルレベルを可変設定自在とすることにより、スクランブルして提供する画像データの画質の劣化レベルを加減することができ、目的・用途に応じたスクランブル画像の提供が可能となる。

#### 【0031】

請求項10記載の発明は、請求項9記載の画像符号化装置において、ビットプレーン化された離散ウェーブレット変換係数であるビット係数のビット位置の選択によりスクランブルレベルが可変設定自在である。

#### 【0032】

従って、J P E G 2 0 0 0 アルゴリズムによれば、画像データの閲覧に際してサブバンド機能等を利用することでサムネイル画像の提供が簡単に行えるが、例えば、ビット係数の上位ビットのデータをランダム化によりスクランブルをかければ、解像度は変わらない状態で画像の形が崩れることによりボケたようなスクランブル、即ち、サムネイル画像への画質劣化の影響を与えやすいスクランブルを実現でき、ビット係数のビット位置の選択によりスクランブルレベルが可変設定自在となる。

#### 【0033】

請求項 11 記載の発明は、請求項 9 記載の画像符号化装置において、離散ウェーブレット変換係数のうちの離散ウェーブレット変換処理によるサブバンドの階層位置の選択によりスクランブルレベルが可変設定自在である。

#### 【0034】

従って、J P E G 2 0 0 0 アルゴリズムによれば、解像度に関してサブバンド階層構造を有し、低階層の L L なるサブバンドが最も解像度の高い部分となるので、例えば、低階層のサブバンド部分のデータをランダム化によりスクランブルをかければ、繊細なスクランブル、即ち、サムネイル画像への画質劣化の影響を与えにくいスクランブルを実現でき、離散ウェーブレット変換処理によるサブバンドの階層位置の選択によりスクランブルレベルが可変設定自在となる。

#### 【0035】

請求項 12 記載の発明は、請求項 9 記載の画像符号化装置において、離散ウェーブレット変換による符号化単位となる複数の矩形領域が集合しスクランブル化が施されるブロックの大きさの選択によりスクランブルレベルが可変設定自在である。

#### 【0036】

従って、J P E G 2 0 0 0 アルゴリズムによれば、画像全体に限らず、符号化単位となる複数の矩形領域（タイル）を単位として処理が可能であるので、例えば、ランダム化によるスクランブル化を行う領域を限定するブロックの大きさを大きくすると、雑然としたスクランブル画像となり、画像中で表現される元の形（画像全体像）が判り難くなるスクランブル、即ち、サムネイル画像への画質劣化の影響を与えやすいスクランブルを実現でき、スクランブル化が施されるブロックの大きさの選択によりスクランブルレベルが可変設定自在となる。

#### 【0037】

請求項 13 記載の発明の符号復号化装置は、請求項 1 ないし 12 の何れか一記載の画像符号化装置によりスクランブル化された符号データの入力を受付ける符号データ入力手段と、入力された符号データを J P E G 2 0 0 0 アルゴリズムに従い画像データに復号する復号化手段と、パスワード入力に基づき前記復号化手段による復号処理において符号データに対するスクランブルを解除するデスクラ



ンブル化手段と、を備える。

【0038】

従って、予めプロバイダ等から提供されたパスワードを含む特別なデスクランブル用のソフトを有する閲覧許可者のみが、スクランブルの影響の残らない元の画像データの閲覧が可能となる。

【0039】

これらの各発明による作用は、各々以下のような画像符号化用プログラム、符号復号化用プログラム又は記憶媒体によっても同様に奏する。

【0040】

請求項14記載の発明の画像符号化用プログラムは、コンピュータにインストールされ、又は、解釈されて、当該コンピュータに、入力された画像データをJPEG2000アルゴリズムに従い圧縮符号化する圧縮符号化機能と、この圧縮符号化機能により可逆圧縮符号化される直前のデータをパスワード入力に基づき解除可能にスクランブル化して可逆圧縮符号化に供するスクランブル化機能と、を実行させる。

【0041】

請求項15記載の発明は、請求項14記載の画像符号化用プログラムにおいて、前記スクランブル化機能は、データのランダム化によりスクランブル化する。

【0042】

請求項16記載の発明は、請求項14又は15記載の画像符号化用プログラムにおいて、スクランブル前のデータとスクランブルデータとの間の差分値をランダム化により復元可能に暗号化した電子透かしデータとしてスクランブル後のデータ中に埋め込む電子透かし埋め込み機能を前記コンピュータに実行させる。

【0043】

請求項17記載の発明は、請求項16記載の画像符号化用プログラムにおいて、電子透かし埋め込み機能は、ランダム化により復元可能に暗号化するための種データとしてパスワードとスクランブル前のデータとを用いる。

**【0044】**

請求項18記載の発明は、請求項14ないし17の何れか一記載の画像符号化用プログラムにおいて、前記圧縮符号化機能は、入力された画像データをJPE G 2 0 0 0 アルゴリズムの可逆モードに従い圧縮符号化するものであり、前記スクランブル化機能は、前記圧縮符号化手段による離散ウェーブレット変換処理前の画像データをスクランブル化する。

**【0045】**

請求項19記載の発明は、請求項14ないし17の何れか一記載の画像符号化用プログラムにおいて、前記圧縮符号化機能は、入力された画像データをJPE G 2 0 0 0 アルゴリズムの非可逆モードに従い圧縮符号化するものであり、前記スクランブル化機能は、前記圧縮符号化手段による離散ウェーブレット変換処理後に量子化された離散ウェーブレット変換係数をスクランブル化する。

**【0046】**

請求項20記載の発明は、請求項19記載の画像符号化用プログラムにおいて、前記スクランブル化機能は、量子化としてビットプレーン化された離散ウェーブレット変換係数であるビット係数の有意係数を対象としてスクランブル化する。

**【0047】**

請求項21記載の発明は、請求項20記載の画像符号化用プログラムにおいて、前記スクランブル化機能は、スクランブル化により対象となるビット係数を反転させる場合には隣り桁のビット係数を反転させる。

**【0048】**

請求項22記載の発明は、請求項19ないし21の何れか一記載の画像符号化用プログラムにおいて、前記スクランブル化機能は、量子化された離散ウェーブレット変換係数に対するスクランブルレベルが可変設定自在である。

**【0049】**

請求項23記載の発明は、請求項22記載の画像符号化用プログラムにおいて、ビットプレーン化された離散ウェーブレット変換係数であるビット係数のビット位置の選択によりスクランブルレベルが可変設定自在である。

**【0050】**

請求項 24 記載の発明は、請求項 22 記載の画像符号化用プログラムにおいて、離散ウェーブレット変換係数のうちの離散ウェーブレット変換処理によるサブバンドの階層位置の選択によりスクランブルレベルが可変設定自在である。

**【0051】**

請求項 25 記載の発明は、請求項 22 記載の画像符号化用プログラムにおいて、離散ウェーブレット変換による符号化単位となる複数の矩形領域が集合しスクランブル化が施されるブロックの大きさの選択によりスクランブルレベルが可変設定自在である。

**【0052】**

請求項 26 記載の発明の符号復号化用プログラムは、コンピュータにインストールされ、又は、解釈されて、当該コンピュータに、請求項 1 ないし 12 の何れか一記載の画像符号化装置によりスクランブル化された符号データの入力を受付ける符号データ入力機能と、入力された符号データを J P E G 2 0 0 0 アルゴリズムに従い画像データに復号する復号化機能と、パスワード入力に基づき前記復号化機能による復号処理において符号データに対するスクランブルを解除するデスクランブル化機能と、を実行させる。

**【0053】**

請求項 27 記載の発明のコンピュータ読取り可能な記憶媒体は、請求項 14 ないし 26 の何れか一記載のプログラムを格納している。

**【0054】****【発明の実施の形態】**

本発明の一実施の形態を図面に基づいて説明する。

**【0055】****[J P E G 2 0 0 0 について概略説明]**

本実施の形態は、J P E G 2 0 0 0 アルゴリズムを利用するものであり、まず、J P E G 2 0 0 0 について概略説明する。

**【0056】**

図 1 は、J P E G 2 0 0 0 方式の基本となる階層符号化アルゴリズムを実現す

るシステムの機能ブロック図である。このシステムは、色空間変換・逆変換部 101、2次元ウェーブレット変換・逆変換部 102、量子化・逆量子化部 103、エントロピー符号化・復号化部 104、タグ処理部 105の各機能ブロックにより構成されている。

#### 【0057】

このシステムが従来の J P E G アルゴリズムと比較して最も大きく異なる点の一つは変換方式である。J P E G では離散コサイン変換 (D C T : Discrete Cosine Transform) を用いているのに対し、この階層符号化アルゴリズムでは、2次元ウェーブレット変換・逆変換部 102において、離散ウェーブレット変換 (D W T : Discrete Wavelet Transform) を用いている。D W T は D C T に比べて、高圧縮領域における画質が良いという長所を有し、この点が、J P E G の後継アルゴリズムである J P E G 2000 で D W T が採用された大きな理由の一つとなっている。

#### 【0058】

また、他の大きな相違点は、この階層符号化アルゴリズムでは、システムの最終段に符号形成を行うために、タグ処理部 105の機能ブロックが追加されていることである。このタグ処理部 105で、画像の圧縮動作時には圧縮データが符号列データとして生成され、伸長動作時には伸長に必要な符号列データの解釈が行われる。そして、符号列データによって、J P E G 2000 は様々な便利な機能を実現できるようになった。例えば、ブロック・ベースでの D W T におけるオクターブ分割に対応した任意の階層 (デコンポジション・レベル) で、静止画像の圧縮伸長動作を自由に停止させることができるようになる (後述する図3参照)。

#### 【0059】

原画像の入出力部分には、色空間変換・逆変換 101が接続される場合が多い。例えば、原色系の R (赤) / G (緑) / B (青) の各コンポーネントからなる R G B 表色系や、補色系の Y (黄) / M (マゼンタ) / C (シアン) の各コンポーネントからなる Y M C 表色系から、Y U V あるいは Y C b C r 表色系への変換又は逆変換を行う部分がこれに相当する。

**【0060】**

次に、J P E G 2 0 0 0 アルゴリズムについて説明する。

**【0061】**

カラー画像は、一般に、図2に示すように、原画像の各コンポーネント111（ここではRGB原色系）が、矩形をした領域によって分割される。この分割された矩形領域は、一般にブロックあるいはタイルと呼ばれているものであるが、J P E G 2 0 0 0 では、タイルと呼ぶことが一般的であるため、以下、このような分割された矩形領域をタイルと記述することにする（図2の例では、各コンポーネント111が縦横4×4、合計16個の矩形のタイル112に分割されている）。このような個々のタイル112（図2の例で、R00, R01, ..., R15 / G00, G01, ..., G15 / B00, B01, ..., B15）が、画像データの圧縮伸長プロセスを実行する際の基本単位となる。従って、画像データの圧縮伸長動作は、コンポーネントごと、また、タイル112ごとに、独立に行われる。

**【0062】**

画像データの符号化時には、各コンポーネント111の各タイル112のデータが、図1の色空間変換・逆変換部101に入力され、色空間変換を施された後、2次元ウェーブレット変換部102で2次元ウェーブレット変換（順変換）が施されて、周波数帯に空間分割される。

**【0063】**

図3には、デコンポジション・レベル数が3の場合の、各デコンポジション・レベルにおけるサブバンドを示している。即ち、原画像のタイル分割によって得られたタイル原画像（0LL）（デコンポジション・レベル0）に対して、2次元ウェーブレット変換を施し、デコンポジション・レベル1に示すサブバンド（1LL, 1HL, 1LH, 1HH）を分離する。そして引き続き、この階層における低周波成分1LLに対して、2次元ウェーブレット変換を施し、デコンポジション・レベル2に示すサブバンド（2LL, 2HL, 2LH, 2HH）を分離する。順次同様に、低周波成分2LLに対しても、2次元ウェーブレット変換を施し、デコンポジション・レベル3に示すサブバンド（3LL, 3HL, 3LH

、3HH)を分離する。図3では、各デコンポジション・レベルにおいて符号化の対象となるサブバンドを、網掛けで表してある。例えば、デコンポジション・レベル数を3としたとき、網掛けで示したサブバンド(3HL, 3LH, 3HH, 2HL, 2LH, 2HH, 1HL, 1LH, 1HH)が符号化対象となり、3LLサブバンドは符号化されない。

#### 【0064】

次いで、指定した符号化の順番で符号化の対象となるビットが定められ、図1に示す量子化・逆量子化部103で対象ビット周辺のビットからコンテキストが生成される。

#### 【0065】

この量子化の処理が終わったウェーブレット係数は、個々のサブバンド毎に、「プレシント」と呼ばれる重複しない矩形に分割される。これは、インプリメンテーションでメモリを効率的に使うために導入されたものである。図4に示したように、一つのプレシントは、空間的に一致した3つの矩形領域からなっている。更に、個々のプレシントは、重複しない矩形の「コード・ブロック」に分けられる。これは、エントロピー・コーディングを行う際の基本単位となる。

#### 【0066】

ウェーブレット変換後の係数値は、そのまま量子化し符号化することも可能であるが、JPEG2000では符号化効率を上げるために、係数値を「ビットプレーン」単位に分解し、画素あるいはコード・ブロック毎に「ビットプレーン」に順位付けを行うことができる。

#### 【0067】

ここで、図5はビットプレーンに順位付けする手順の一例を示す説明図である。図5に示すように、この例は、原画像(32×32画素)を16×16画素のタイル4つで分割した場合で、デコンポジション・レベル1のプレシントとコード・ブロックの大きさは、各々8×8画素と4×4画素としている。プレシントとコード・ブロックの番号は、ラスタ順に付けられており、この例では、プレシントが番号0から3まで、コード・ブロックが番号0から3まで割り当てられている。タイル境界外に対する画素拡張にはミラーリング法を使い、可逆

(5, 3) フィルタでウェーブレット変換を行い、デコンポジション・レベル 1 のウェーブレット係数値を求めている。

#### 【0068】

また、タイル 0 / プレシント 3 / コード・ブロック 3 について、代表的な「レイヤ」構成の概念の一例を示す説明図も図 5 に併せて示す。変換後のコード・ブロックは、サブバンド (1LL, 1HL, 1LH, 1HH) に分割され、各サブバンドにはウェーブレット係数値が割り当てられている。

#### 【0069】

レイヤの構造は、ウェーブレット係数値を横方向 (ビットプレーン方向) から見ると理解し易い。1つのレイヤは任意の数のビットプレーンから構成される。この例では、レイヤ 0, 1, 2, 3 は、各々、1, 3, 1, 3 のビットプレーンから成っている。そして、LSB (Least Significant Bit: 最下位ビット) に近いビットプレーンを含むレイヤ程、先に量子化の対象となり、逆に、MSB (Most Significant Bit: 最上位ビット) に近いレイヤは最後まで量子化されずに残ることになる。LSB に近いレイヤから破棄する方法はトランケーションと呼ばれ、量子化率を細かく制御することが可能である。このように、ビットプレーン (又はサブビットプレーン) を削っていない状態の符号から所定の圧縮率になるまで符号を破棄する処理はポスト量子化と呼ばれており、JPEG 2000 アルゴリズムの最も大きな特徴である。

#### 【0070】

図 1 に示すエントロピー符号化・復号化部 104 では、コンテキストと対象ビットから確率推定によって、各コンポーネント 111 のタイル 112 に対する符号化を行う。こうして、原画像の全てのコンポーネント 111 について、タイル 112 単位で符号化処理が行われる。最後にタグ処理部 105 は、エントロピー符号化・復号化部 104 からの全符号化データを 1 本の符号列データ (コードストリーム) に結合するとともに、それにタグを付加する処理を行う。

#### 【0071】

図 6 には、この符号列データの 1 フレーム分の概略構成を示している。この符号列データの先頭と各タイルの符号データ (bit stream) の先頭にはヘッダ (メ

インヘッダ (Main header)、タイル境界位置情報やタイル境界方向情報等であるタイルパートヘッダ (tile part header) ) と呼ばれるタグ情報が付加され、その後に、各タイルの符号化データが続く。なお、メインヘッダ (Main header) には、符号化パラメータや量子化パラメータが記述されている。そして、符号列データの終端には、再びタグ (end of codestream) が置かれる。

#### 【0072】

一方、復号化時には、画像データの符号化時とは逆に、各コンポーネント 111 の各タイル 112 の符号列データから画像データを生成する。この場合、タグ処理部 105 は、外部より入力した符号列データに付加されたタグ情報を解釈し、符号列データを各コンポーネント 111 の各タイル 112 の符号列データに分解し、その各コンポーネント 111 の各タイル 112 の符号列データ毎に復号化処理 (伸長処理) を行う。このとき、符号列データ内のタグ情報に基づく順番で復号化の対象となるビットの位置が定められるとともに、量子化・逆量子化部 103 で、その対象ビット位置の周辺ビット (既に復号化を終えている) の並びからコンテキストが生成される。エントロピー符号化・復号化部 104 で、このコンテキストと符号列データから確率推定によって復号化を行い、対象ビットを生成し、それを対象ビットの位置に書き込む。このようにして復号化されたデータは周波数帯域毎に空間分割されているため、これを 2 次元ウェーブレット変換・逆変換部 102 で 2 次元ウェーブレット逆変換を行うことにより、画像データの各コンポーネントの各タイルが復元される。復元されたデータは色空間変換・逆変換部 101 によって元の表色系の画像データに変換される。

#### 【0073】

##### [画像符号化装置、符号復号化装置]

本実施の形態の画像符号化装置、符号復号化装置は、その一例として、インターネット等のネットワークを利用してプロバイダから各ユーザに画像データ (デジタルコンテンツ) を配布するシステム構成を想定しており、配布元となるプロバイダのコンピュータを画像符号化装置、配布先となる各ユーザのコンピュータを符号復号化装置とする例である。

#### 【0074】



図7はこのようなシステムを示す概略システム構成図であり、プロバイダの画像符号化装置となるサーバコンピュータ1にはインターネット等のネットワーク2を介して各ユーザの符号復号化装置となるパーソナルコンピュータ3が接続可能とされている。

#### 【0075】

図8は、これらのサーバコンピュータ1やパーソナルコンピュータ3のハードウェア構成を概略的に示すブロック図である。図8に示すように、コンピュータ1, 3は、当該コンピュータの主要部であって各部を集中的に制御するCPU (Central Processing Unit) 6を備えている。このCPU 6には、BIOSなどを記憶した読出し専用メモリであるROM (Read Only Memory) 7と、各種データを書換え可能に記憶するRAM (Random Access Memory) 8とがバス9で接続されている。RAM 8は、各種データを書換え可能に記憶する性質を有していることから、CPU 6の作業エリアとして機能し、例えば入力バッファ等の役割を果たす。

#### 【0076】

さらにバス9には、HDD (Hard Disk Drive) 10と、配布されたプログラムであるコンピュータソフトウェアを読み取るための機構としてCD (Compact Disc) -ROM 11を読み取るCD-ROMドライブ12と、相手方となるコンピュータ3又は1とネットワーク5との通信を司る通信制御装置13と、キーボードやマウスなどの入力装置14と、CRT (Cathode Ray Tube) やLCD (Liquid Crystal Display) である表示装置15とが、図示しないI/Oを介して接続されている。

#### 【0077】

そして、パーソナルコンピュータ3の場合であれば、ネットワーク5を介してサーバコンピュータ1からダウンロードした圧縮符号化された符号データは、HDD 10に格納されることになる。

#### 【0078】

また、CD-ROM 11は、本発明の記憶媒体を実施するものであり、OS (Operating System) や各種コンピュータソフトウェアが記憶されている。CPU

6は、CD-ROM11に記憶されているコンピュータソフトウェアをCD-ROMドライブ12で読み取り、HDD10にインストールする。

#### 【0079】

なお、記憶媒体としては、CD-ROM11のみならず、DVDなどの各種の光ディスク、各種光磁気ディスク、FDなどの各種磁気ディスク等、半導体メモリ等の各種方式のメディアを用いることができる。また、通信制御装置13を介してインターネットなどのネットワーク5からコンピュータソフトウェアをダウンロードし、HDD10にインストールするようにしてもよい。この場合に、送信側のサーバでコンピュータソフトウェアを記憶している記憶装置も、本発明の記憶媒体である。なお、コンピュータソフトウェアは、所定のOS (Operating System) 上で動作するものであってもよいし、その場合に後述の各種処理の一部の実行をOSに肩代わりさせるものであってもよいし、所定のアプリケーションソフトやOSなどを構成する一群のプログラムファイルの一部として含まれているものであってもよい。

#### 【0080】

このような構成のコンピュータ1, 3のHDD10には、コンピュータソフトウェアの一つとして、画像を処理する画像処理プログラムが記憶されている。この画像処理プログラムは本発明のプログラムを実施するものである。そして、この画像処理プログラムに基づいてCPU6が実行する処理により、コンピュータ1, 3の各部の各種機能を実現する。その一つとして、図1を参照して説明したJPEG2000アルゴリズムの各機能ブロックを備え、前述のようなJPEG2000アルゴリズムにより画像データの圧縮符号化、又は、符号データの復号化を行う。即ち、図1に示したような圧縮符号化手段及び復号化手段の機能は、HDD10に記憶されているプログラムに基づいてCPU6が行う処理により実行される（もっとも、論理回路等を利用したハードウェア構成により実行させてもよい）。

#### 【0081】

[サーバコンピュータにおけるスクランブル画像符号化処理]

前述したように、JPEG2000アルゴリズムによれば、画像データの符号

化に際しては、入力された画像データをウェーブレット変換した結果の離散ウェーブレット変換係数を量子化するまでは、可逆又は非可逆な変換過程をとることができ、量子化の処理が終わった離散ウェーブレット変換係数からエントロピー符号化等の符号列データを生成するまでは可逆変換過程となる。また、符号データの復号化に際して、入力された（圧縮保存済みの）符号列データから離散ウェーブレット変換係数データ（又は、量子化係数データ：可逆圧縮の場合は量子化しないため）を復号化するまでは、可逆変換過程を経ることとなり、復号化した離散ウェーブレット変換係数データから画像データを生成するまでは可逆又は非可逆な変換過程をとることができる。

#### 【0082】

ここに、本実施の形態のサーバコンピュータ 1 は、例えば J P E G 2 0 0 0 アルゴリズムの非可逆モードにより画像データを圧縮符号化するものとし、かつ、その圧縮符号化の際に必要なに応じてスクランブル化処理を行って符号データを生成するものである。

#### 【0083】

サーバコンピュータ 1 においてこのような画像符号化処理を行う J P E G 2 0 0 0 アルゴリズムによる圧縮符号化手段を適宜簡略化して書き直すと、図 9 のように示すことができる。即ち、非可逆処理を離散ウェーブレット変換係数の量子化段階で行うものであり、スキャナ、デジタルカメラ、パソコン等の各種機器から処理対象となる画像データの入力を受付ける入力部 2 1、受付けた画像データに対して色空間変換等の処理を経た後、2 次元ウェーブレット変換処理を行う 2 次元ウェーブレット変換部 2 2（1 0 2 に相当）、変換された離散ウェーブレット変換係数に対して効率のよい圧縮を行うためにそのダイナミックレンジを削減するポスト量子化等の非可逆な量子化処理を行う係数量子化部 2 3（1 0 3 に相当）、量子化された離散ウェーブレット変換係数に対して前述のエントロピー符号化（係数モデリング＋算術符号化）等の可逆圧縮符号化処理を行う可逆圧縮符号化部 2 4（1 0 4 に相当）、符号化された符号データの並べ替え処理等を行い、必要箇所に出力する符号データ出力部 2 5（1 0 5 に相当）による圧縮符号化手段 2 6 を有する。

## 【0084】

加えて、この圧縮符号化手段 26 により可逆圧縮符号化される直前のデータ、ここでは、係数量子化部 23 により量子化された離散ウェーブレット変換係数をスクランブル化するスクランブル化手段又はスクランブル化機能として作用するスクランブル化部 27 と、スクランブル化されたデータを復元するためのデータを電子透かしデータとしてスクランブル後のデータ中に埋め込む電子透かし埋め込み手段又は電子透かし埋め込み機能として作用する電子透かし埋め込み部 28 とが付加されている。このようなスクランブル化部 27 は入力部 21 に対して画像データとともに所定のパスワード（英数字等による複数桁の暗証番号等）が入力された場合にのみ機能するものであり、入力されたパスワードは暗号化されてスクランブル化に供される。従って、画像データ入力に際してパスワードが入力されない場合には、スクランブル化部 27 及び電子透かし埋め込み部 28 の処理を経ることなく、可逆圧縮符号化処理に移行する。

## 【0085】

ここで、スクランブル化部 27 での処理について説明する。このスクランブル化部 27 はランダム化によりデータのスクランブル化を行うものである。即ち、スクランブル前の元のデータに対してハッシュ（Hash）関数に基づくハッシュ変換を施して乱数暗号化（ランダム化）することにより、スクランブル前の元のデータを解読できないようにするものである。このハッシュ関数は、引数を種（タネ）にして生成する一方向性の乱数発生関数であり、

性質 1；出力値から入力値は推測できない

性質 2；入力値が 1 ビットでも変わると、出力値は全面的に変化する

性質 3；同じ出力になる異なる 2 つの入力の探索は現実的には不可能

なる性質を有している（出典；電子情報通信学会誌 2000 年 2 月“公平性保証とプライバシー保護”佐古和恵）。

## 【0086】

このようにハッシュ変換は、生成後のデータから元のデータを推定することが不可能であるため、データのスクランブル化に際してハッシュ変換を用いることにより、その解読を防止することができる。

## 【0087】

電子透かし埋め込み部28による電子透かしの埋め込みは、スクランブル化されたデータを復号する際にパスワードを含む専用のソフトウェアにより元のデータへの復元を可能にするための処理であり、ここでは、スクランブルデータとスクランブル前のデータとの差分値（ずらし量）をハッシュ関数を用いたランダムイズで復元できるように暗号化した電子透かしデータとして、画像全体のスクランブル後のデータ（ここでは、量子化・スクランブル化された離散ウェーブレット変換係数）中に埋め込むものである。

## 【0088】

ここで、ランダムイズで復元可能な暗号化の方法の一例を簡単に説明する。まず、ハッシュ変換の方法の一例を、

$$[\text{変換結果データ}] = [\text{変換元データ}] * [\text{生成元}] \% [\text{法：素数}]$$

$$[\text{変換元データ}] = [\text{変換結果データ}] - 1 * [\text{生成元}] \% [\text{法：素数}]$$

とした場合、その暗号化の例としては、

[元Data：10進数]            [変換内容：bit]

0                                : 11111111

1～126                        : 先頭1bitはON“1”で、後続の7bitは10進数1  
                                     ～126をハッシュ変換したデータ

127                             : 10000000

128                             : 01111111

129～254                    : 先頭1bitはOFF“0”で、後続の7bitは10進数  
                                     129～254を－128してからハッシュ変換し  
                                     て1～126にしたデータをbitで表現したもの

255                             : 00000000

が挙げられる。従って、具体的なハッシュ変換例を例示すると、

$$[\text{法：素数}] = 127$$

$$[\text{生成元}] = 3$$

$$[\text{変換元データ}] = 0x20010831 \text{ (日付：2001年8月31日)}$$

< [変換結果データ] 使用の変換 >

変換後data: 0xE0839894

< [変換結果データ] - 1 使用の変換 >

変換後data: 0xB5D5ADE5

[逆変換後データ] = 0x20010831 (日付: 2001年8月31日)

となり、復元される。暗号化には、周知のRSAなどの公開鍵方式を利用してもよい。

### 【0089】

ハッシュ変換を用いたスクランブル化処理時の元のデータからのずらし量（差分値）の決定方法の、より具体的な例について説明する。

### 【0090】

いま、

$R_k = \text{Hash}(\text{“パスワード”}, \text{“直前}(k-1)\text{番目の処理済値”})$  の  
最下位ビットを除いた値

$P_k = \text{Hash}(\text{“パスワード”}, \text{“直前}(k-1)\text{番目の処理済値”})$  の  
最下位ビット  $\rightarrow$  ON:  $\ast(-1)$ , OFF:  $\ast(+1)$

とすると ( $P_k$  に関する式中の処理済値とは、順次処理 (画素の並び) における直前の処理結果 (ずらし処理墨の量子化データ) である)、

$(\text{ずらし量}) = R_k \ast (\text{程度因子}) \ast P_k$

で表される。具体的な数値例を示すと、表1に示すような量子化データの並びの場合、

### 【0091】

【表1】

①	k-1	k	k+1	k+2
②	11	19	23	20
③	$(+2) \ast 2$	$(-3) \ast 2$	$(-1) \ast 2$	$(+1) \ast 2$

### 【0092】

ただし、表1中、①は処理順序No. ②は元の量子化データ、③はスクラ  
ン

ブル用増減値（ずらし量）＊（程度因子：2）である。

【0093】

$R_k = \text{Hash}(\text{“パスワード”}, (11+2*2)) = 7 \rightarrow 3$ （最下位ビットを除いた値）

$P_k = \text{Hash}(\text{“パスワード”}, (11+2*2)) = 7 \rightarrow -1$ （最下位ビットがON）

（ずらし量） $= 3 * (\text{程度因子：2}) * (-1) = -6$

となる。

【0094】

このように離散ウェーブレット変換係数はスクランブル化され、復元のための暗号化された電子透かしデータが埋め込まれたデータ（離散ウェーブレット変換係数）に対して可逆圧縮符号化部24によって可逆変換を施すことにより、スクランブル化され、かつ、電子透かしデータが埋め込まれた離散ウェーブレット変換係数を劣化させることなく圧縮させることができる。この後、タグ処理等が施された符号データは、HDD10等のメモリに保存される。

【0095】

このように、本実施の形態によれば、サーバコンピュータ1において、入力された画像データをJPEG2000アルゴリズムの非可逆モードに従い圧縮符号化する場合であっても、量子化処理の後の圧縮符号化処理は可逆的な処理となるので、その直前のデータである離散ウェーブレット変換処理後の量子化された離散ウェーブレット変換係数にスクランブルをかけても、データを劣化させることなく圧縮させることができるので、そのスクランブルも可逆的に完全に復号させることで、完全にスクランブルの影響をなくすることが可能となる。そして、このようなスクランブルデータを元のデータに復元するためのデータが暗号化された電子透かしデータとして画像全体に埋め込まれているので、不特定多数の利用者によるスクランブル解除のための解読を事実上不可能にし、スクランブル前の元データの保護を図ることができる。

【0096】

ところで、スクランブル化部27で乱数暗号化するデータの対象としては、離散ウェーブレット変換係数の最上位係数を避け、下位係数を主体に行うことが望ましい。上位係数ほど元の画像データに近いものであり、このような係数を対象

にランダム化すると、暗号化の程度が大きくなり、スクランブル画像から元の画像を全く想像できなくなってしまうからである。もっとも、最上位係数しかない場合には、最上位係数を乱数暗号化の対象とする。

#### 【0097】

より具体的には、量子化としてビットプレーン化されたビット係数（離散ウェーブレット変換係数）の有意係数を対象としてスクランブル化すればよい。「ビット係数の有意係数」とは、例えば前述の J P E G 2 0 0 0 アルゴリズム中で説明したようにビット表現した処理対象となるビットプレーン化された離散ウェーブレット変換係数を上位ビットから下位ビット方向に符号化する場合に、注目するビット係数が 0 でないことが判っている係数をいう。このようなビットプレーン化されたビット係数の有意係数を対象としてスクランブル化することで、効果的なスクランブルをかけることができる。

#### 【0098】

この場合のスクランブル化処理例として、対象となるビット係数を反転させる方式（“0” → “1” に反転、又は、“1” → “0” に反転）を採ることができる。このようなビット係数反転方式を採る場合、その隣り桁（直上桁又は直下桁）のビット係数も併せて反転させることが望ましい。即ち、“0” → “1” に反転であれば、“1” → “0” に反転し、“1” → “0” に反転であれば、“0” → “1” に反転する。これは、スクランブル化により対象となるビット係数を反転させる場合には、そのビット係数の反転処理よりこの部分で極端に表示画像の明るさが変わってしまい画質劣化することがあるので、この画質劣化への影響を軽減・緩和させるためである。もっとも、この場合もあまりスクランブルをかけすぎると元の画像が判らなくなってしまうので、このような場合には、直下桁側の隣り桁のみ反転させることが望ましい。

#### 【0099】

また、スクランブル化部 27 による量子化データ（離散ウェーブレット変換係数）のスクランブル処理に際しては、J P E G 2 0 0 0 の特徴を利用することにより、そのスクランブルレベル（従って、画質劣化レベル）を任意に可変設定することができるので、プロバイダが提供する画像データの目的・用途に応じて適



宜スクランブルレベルを設定することにより、画質劣化レベルを加減したスクランブル画像を提供することができる。

#### 【0100】

このようなスクランブルレベルを可変設定する一例としては、J P E G 2 0 0 0 アルゴリズムにおける図 5 中に示したようなビットプレーン処理を利用することができる。つまり、J P E G 2 0 0 0 アルゴリズムによれば、画像データの閲覧に際してサブバンド機能等を利用することでサムネイル画像の提供が簡単に行えるが、例えば、ビットプレーンにおけるビット係数の上位ビットのデータをランダム化によりスクランブルをかければ、解像度は変わらない状態で画像の形が崩れることによりボケたようなスクランブル、即ち、サムネイル画像への画質劣化の影響を与えやすいスクランブルを実現できる。よって、ビットプレーンにおけるビット係数のビット位置の選択によりスクランブルレベルが可変設定自在となる。

#### 【0101】

スクランブルレベルを可変設定する他例としては、J P E G 2 0 0 0 アルゴリズムの離散ウェーブレット変換処理によるサブバンド構造を利用することができる。J P E G 2 0 0 0 アルゴリズムによれば、解像度に関して図 3 等 に示したようなサブバンド階層構造を有し、低階層の L L ( 3 L L , 2 L L , 1 L L 等 ) なるサブバンドが最も解像度の高い部分となるので、例えば、低階層のサブバンド部分のデータをランダム化によりスクランブルをかければ、繊細なスクランブル、即ち、サムネイル画像への画質劣化の影響を与えにくいスクランブルを実現できる。よって、離散ウェーブレット変換処理によるサブバンドの階層位置の選択によりスクランブルレベルが可変設定自在となる。

#### 【0102】

スクランブルレベルを可変設定するさらに他例としては、J P E G 2 0 0 0 アルゴリズムにおける処理単位を利用することができる。J P E G 2 0 0 0 アルゴリズムによれば、図 4 等で前述したように、画像全体に限らず、符号化単位となる複数の矩形領域 ( タイル ) を単位として処理が可能であるので、例えば、ランダム化によるスクランブル化を行う領域を限定するブロックの大きさを大きく

すると、雑然としたスクランブル画像となり、画像中で表現される元の形（画像全体像）が判り難くなるスクランブル、即ち、サムネイル画像への画質劣化の影響を与えやすいスクランブルを実現できる。よって、スクランブル化が施されるブロックの大きさの選択によりスクランブルレベルが可変設定自在となる。

#### 【0103】

[パーソナルコンピュータにおけるスクランブル符号復号化処理]

本実施の形態のパーソナルコンピュータ3は、プロバイダであるサーバコンピュータ1から配布される符号データをJ P E G 2 0 0 0アルゴリズムの非可逆モードにより復号化するものとし、かつ、プロバイダにより閲覧許可されたユーザであれば、復号時にスクランブルを解除するためのパスワードを含むソフトウェアの配布を受けており、その復号化の際にパスワード入力により電子透かしデータを解読してデスクランブル化処理を行って元の画像データを復元するものである。

#### 【0104】

パーソナルコンピュータ3においてこのような符号復号化処理を行うJ P E G 2 0 0 0アルゴリズムによる復号化手段を適宜簡略化して書き直すと、図10のように示すことができる。即ち、サーバコンピュータ1からネットワーク2を通じて配布される前述のようにスクランブル化された符号データの入力を受付ける符号データ入力手段又は符号データ入力機能として作用する入力部31に対して、受付けた符号データに対してエントロピー復号化処理等の可逆圧縮符号の復号化処理を行う可逆圧縮符号の復号化部32、2次元ウェーブレット逆変換等を行って元の画像データに復元する2次元ウェーブレット逆変換部33（103, 102, 101等に相当）による復号化手段34を有する。

#### 【0105】

加えて、復号化部32と2次元ウェーブレット逆変換部33との間には、符号データ中に埋め込まれている電子透かしデータを解読するための電子透かし解読部35と、解読された電子透かしデータに基づき符号データのスクランブルを解除するデスクランブル化手段又はデスクランブル化機能として作用するスクランブル解除部36とが付加されている。このような電子透かし解読部35やスクラ

ンブル解除部 36 は、入力部 31 に対して符号データとともに所定のパスワードが入力された場合のみ機能するものであり、入力されたパスワードに基づき電子透かし解読部 35 で符号データ中に埋め込まれている電子透かしデータを解読し、解読された電子透かしデータ中の差分値データ等に基づきスクランブル解除部 36 で符号データのスクランブルを解除する。従って、プロバイダから閲覧許可されてそのための専用ソフトが配給されていない通常の J P E G 2 0 0 0 アルゴリズムのみの復号化ソフトによる復号処理では、スクランブル化され、かつ、所定の電子透かしデータが埋め込まれて配布される符号データを解読・デスクランブル化することができず、スクランブル化された符号データを元の画像データに復元することはできない。

#### 【0106】

前述のハッシュ変換を用いたスクランブル化処理時の元のデータからのずらし量（差分値）の決定方法に対応する、パーソナルコンピュータ 3 側での復号時の戻し量の決定方法の、具体的な例について説明する。

#### 【0107】

いま、

$R_k = \text{Hash}(\text{“パスワード”}, \text{“復元前の直前}(k-1)\text{番目の量子化データ値”})$

の最下位ビットを除いた値

$P_k = \text{Hash}(\text{“パスワード”}, \text{“復元前の}(k-1)\text{番目の量子化データ値”})$  の  
最下位ビット  $\rightarrow \text{ON} : *(-1)$ ,  $\text{OFF} : *(+1)$

とすると（ $P_k$  に関する式中の復元前の量子化データ値とは、順次処理（画素の並び）における直前の量子化データの復元前データ（ずらし状態のままの量子化データ）である）、

$(\text{戻し量}) = -(\text{ずらし量}) = R_k * (\text{程度因子}) * P_k * (-1)$

で表される。具体的な数値例を示すと、前述の表 1 に示すような量子化データの並びの場合、前述のずらし量決定の場合と同様に、

$R_k = 3$ （最下位ビットを除いた値）

$P_k = -1$ （最下位ビットが ON）

(戻し量) = - (ずらし量) =  $3 * (\text{程度因子: } 2) * (-1) * (-1) = +6$  となる。

#### 【0108】

##### [変形例]

図9では、サーバコンピュータ1が、例えばJPEG2000アルゴリズムの非可逆モードにより画像データを圧縮符号化するものとして説明したが、JPEG2000アルゴリズムの可逆モードにより画像データを圧縮符号化する場合であれば、図11に示すように、スクランブル化部27及び電子透かし埋め込み部28を2次元ウェーブレット変換部22の前段に設け、離散ウェーブレット変換処理前の画像データをスクランブル化し、かつ、電子透かしデータを埋め込むようにしてもよい。

#### 【0109】

即ち、入力された画像データをJPEG2000アルゴリズムの可逆モードに従い圧縮符号化する場合であれば、離散ウェーブレット変換処理前の画像データであっても可逆的に完全に復号されるので、この時点の画像データにスクランブルをかけ、かつ、電子透かしデータを埋め込んでも、可逆的に完全に復号させることができるからである。

#### 【0110】

##### 【発明の効果】

請求項1、14記載の発明によれば、可逆圧縮符号化される直前のデータをパスワード入力に基づき解除可能にスクランブル化した後、当該入力された画像データはJPEG2000アルゴリズムに従い圧縮符号化させるようにしたので、復号に際してもスクランブルデータまでは劣化することなく必ず可逆圧縮符号化により完全に元の状態に戻すことができ、当該スクランブルの影響が残らないスクランブル解除を行うことができ、また、パスワード入力に基づき解除可能なスクランブル化であり、スクランブル解除には所定のパスワード入力を必要とし、当該画像データの閲覧許可者のみへの公開を実現することができる。

#### 【0111】

請求項2、15記載の発明によれば、請求項1又は14記載の発明において、

データ列の並べ換え方式等のような境界線の不透明の問題を伴うことなく、データを適正にスクランブルさせることができる。

【0112】

請求項 3, 16 記載の発明によれば、請求項 1, 2, 14 又は 15 記載の発明において、このような暗号化した電子透かしデータをスクランブル後のデータ中に埋め込むようにしたので、特別なソフト実行のみによりスクランブル前の元のデータの復元を可能にすることができる。

【0113】

請求項 4, 17 記載の発明によれば、請求項 3, 16 記載の発明において、埋め込まれる電子透かしを第三者に解読しにくくさせることができ、スクランブル化されたデータを元に戻すための電子透かしデータの安全性を向上させることができる。

【0114】

請求項 5, 18 記載の発明によれば、請求項 1 ないし 4, 14 ないし 17 の何れか一記載の発明において、入力された画像データを J P E G 2 0 0 0 アルゴリズムの可逆モードに従い圧縮符号化する場合であれば、離散ウェーブレット変換処理前の画像データであっても劣化することなく可逆的に完全に復号されるので、この時点の画像データにスクランブルをかけてもそのスクランブルも可逆的に完全に復号させることで、完全にスクランブルの影響をなくすることができる。

【0115】

請求項 6, 19 記載の発明によれば、請求項 1 ないし 4, 14 ないし 17 の何れか一記載の発明において、入力された画像データを J P E G 2 0 0 0 アルゴリズムの非可逆モードに従い圧縮符号化する場合であっても、量子化処理の後には可逆的な処理となるので、その直前のデータである離散ウェーブレット変換処理後に量子化された離散ウェーブレット変換係数にスクランブルをかけてもそのスクランブルも可逆的に完全に復号させることで、完全にスクランブルの影響をなくすることができる。

【0116】

請求項 7, 20 記載の発明によれば、請求項 6, 19 記載の発明において、こ

のようなビットプレーン化された離散ウェーブレット変換係数であるビット係数の有意係数を対象としてスクランブル化することで、効果的なスクランブルをかけることができる。

#### 【0117】

請求項 8, 21 記載の発明によれば、請求項 7, 20 記載の発明において、スクランブル化により対象となるビット係数を反転させる場合には、そのビット係数の反転処理よりこの部分で極端に表示画像の明るさが変わってしまうことがあるが、併せて、直上桁又は直下桁なる隣り桁のビット係数を反転させることで、緩和させることができる。

#### 【0118】

請求項 9, 22 記載の発明によれば、請求項 6, 8, 19 又は 20 記載の発明において、量子化された離散ウェーブレット変換係数に対するスクランブルレベルを可変設定自在としたので、スクランブルして提供する画像データの画質の劣化レベルを加減することができ、目的・用途に応じたスクランブル画像を提供することができる。

#### 【0119】

請求項 10, 23 記載の発明によれば、請求項 9, 22 記載の発明において、J P E G 2 0 0 0 アルゴリズムによれば、画像データの閲覧に際してサブバンド機能等を利用することでサムネイル画像の提供が簡単に行えるが、例えば、ビット係数の上位ビットのデータをランダム化によりスクランブルをかければ、解像度は変わらない状態で画像の形が崩れることによりボケたようなスクランブル、即ち、サムネイル画像への画質劣化の影響を与えやすいスクランブルを実現でき、ビット係数のビット位置の選択によりスクランブルレベルが可変設定自在となる。

#### 【0120】

請求項 11, 24 記載の発明によれば、請求項 9, 22 記載の発明において、J P E G 2 0 0 0 アルゴリズムによれば、解像度に関してサブバンド階層構造を有し、低階層の L L なるサブバンドが最も解像度の高い部分となるので、例えば、低階層のサブバンド部分のデータをランダム化によりスクランブルをかけ

れば、繊細なスクランブル、即ち、サムネイル画像への画質劣化の影響を与えにくいスクランブルを実現でき、離散ウェーブレット変換処理によるサブバンドの階層位置の選択によりスクランブルレベルが可変設定自在となる。

#### 【0121】

請求項12, 25記載の発明によれば、請求項9, 22記載の発明において、J P E G 2 0 0 0 アルゴリズムによれば、画像全体に限らず、符号化単位となる複数の矩形領域（タイル）を単位として処理が可能であるので、例えば、ランダムサイズによるスクランブル化を行う領域を限定するブロックの大きさを大きくすると、雑然としたスクランブル画像となり、画像中で表現される元の形（画像全体像）が判り難くなるスクランブル、即ち、サムネイル画像への画質劣化の影響を与えやすいスクランブルを実現でき、スクランブル化が施されるブロックの大きさの選択によりスクランブルレベルが可変設定自在となる。

#### 【0122】

請求項13, 26記載の発明によれば、予めプロバイダ等から提供されたパスワードを含む特別なデスクランブル用のソフトを有する閲覧許可者のみが、スクランブルの影響の残らない元の画像データの閲覧が可能となる。

#### 【0123】

請求項27記載の発明によれば、請求項14ないし26の何れか一記載の発明と同様な効果を奏することができる。

#### 【図面の簡単な説明】

##### 【図1】

本発明の前提となる J P E G 2 0 0 0 方式の基本となる階層符号化アルゴリズムを実現するシステムの機能ブロック図である。

##### 【図2】

原画像の各コンポーネントの分割された矩形領域を示す説明図である。

##### 【図3】

デコンポジション・レベル数が3の場合の、各デコンポジション・レベルにおけるサブバンドを示す説明図である。

##### 【図4】

プレシントを示す説明図である。

【図 5】

ビットプレーンに順位付けする手順の一例を示す説明図である。

【図 6】

符号列データの 1 フレーム分の概略構成を示す説明図である。

【図 7】

本発明の一実施の形態のシステムを示すシステム構成図である。

【図 8】

コンピュータのハードウェア構成を概略的に示すブロック図である。

【図 9】

サーバコンピュータにおける画像圧縮符号化の処理系を書き直して示す機能的ブロック図である。

【図 10】

パーソナルコンピュータにおける符号復号化の処理系を書き直して示す機能的ブロック図である。

【図 11】

サーバコンピュータにおける画像圧縮符号化の処理系の変形例を示す機能的ブロック図である。

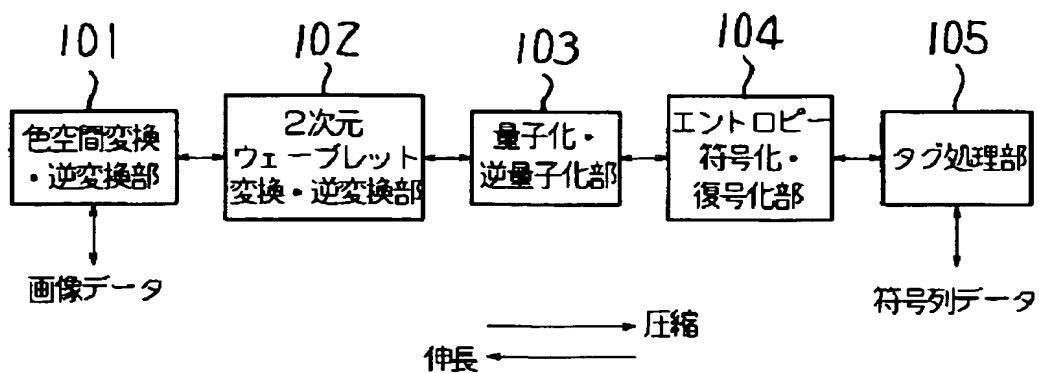
【符号の説明】

- 1        画像符号化装置
- 3        符号復号化装置
- 2 6      圧縮符号化手段、圧縮符号化機能
- 2 7      スクランブル化手段、スクランブル化機能
- 2 8      電子透かし埋め込み手段、電子透かし埋め込み機能
- 3 1      符号データ入力手段、符号データ入力機能
- 3 4      復号化手段、復号化機能
- 3 6      デスクランブル化手段、デスクランブル化機能

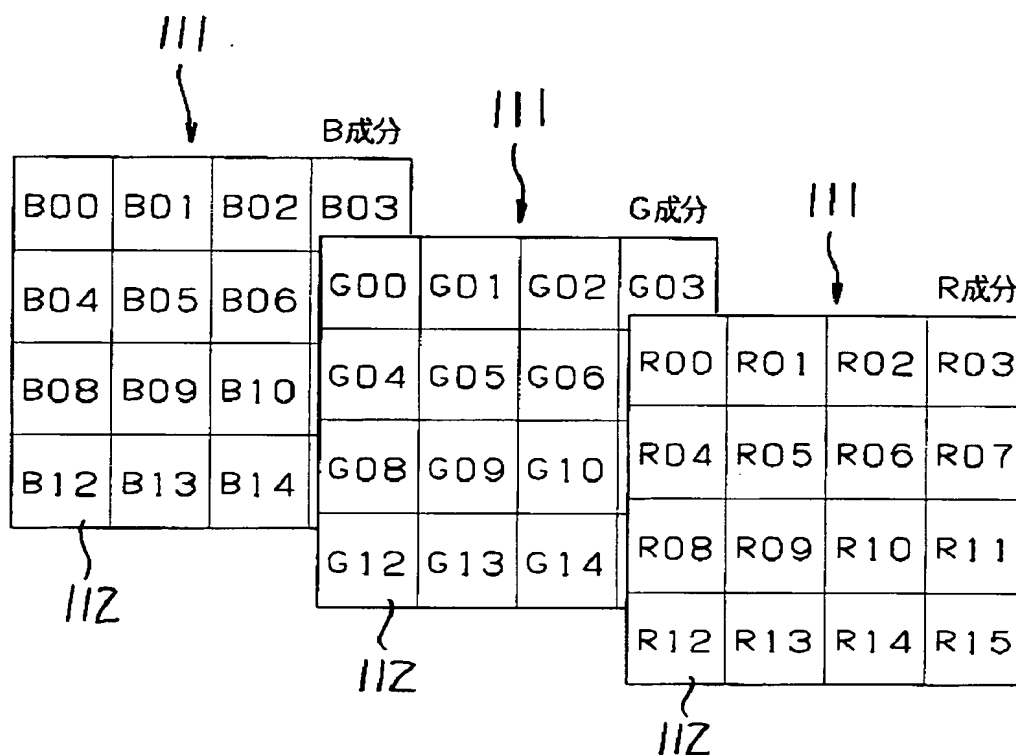


【書類名】 図面

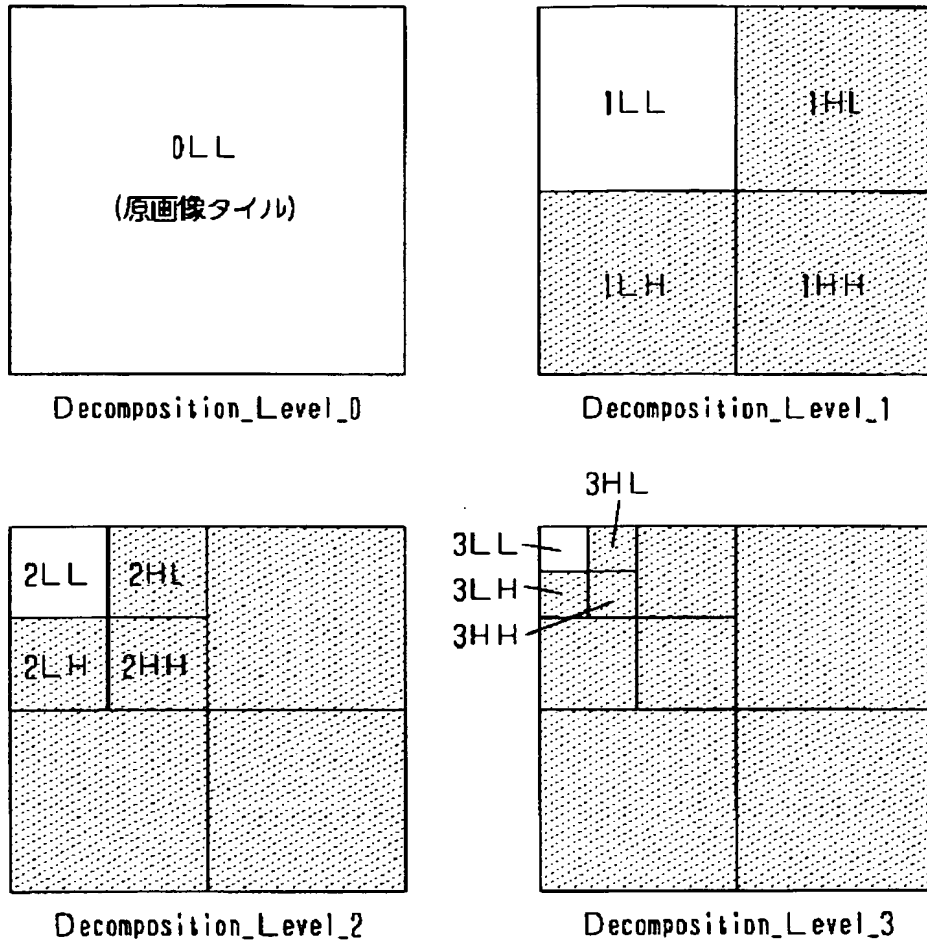
【図 1】



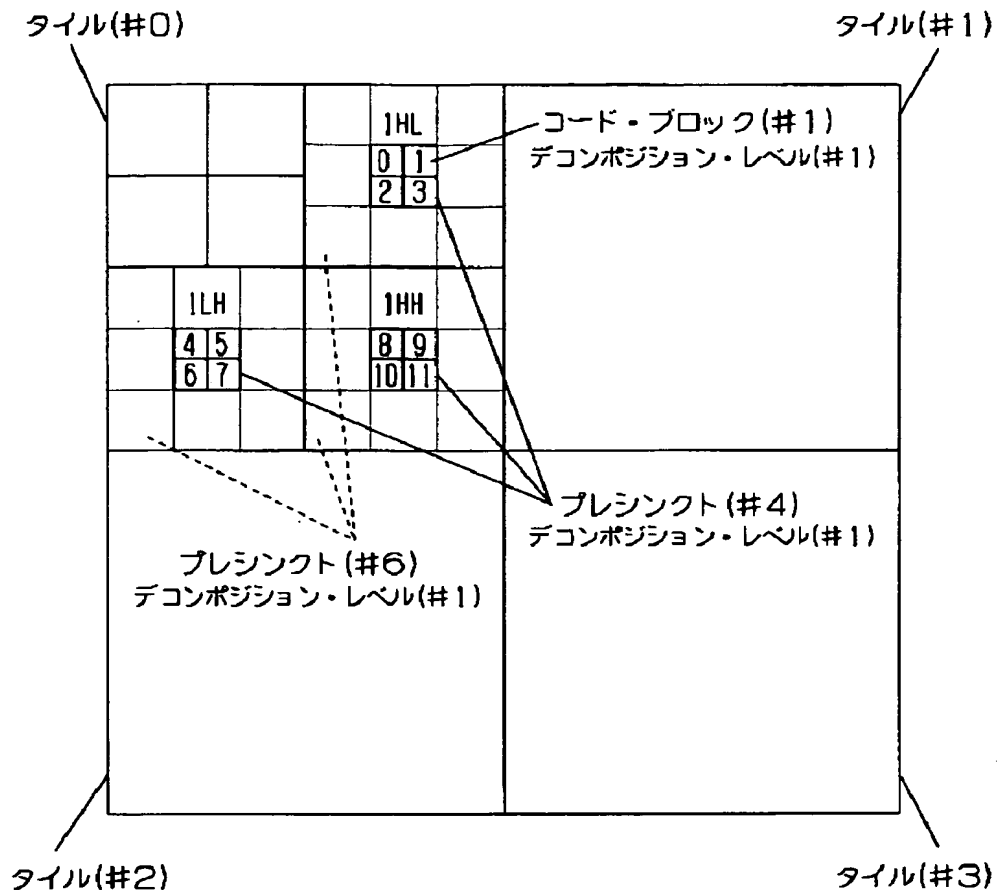
【図 2】



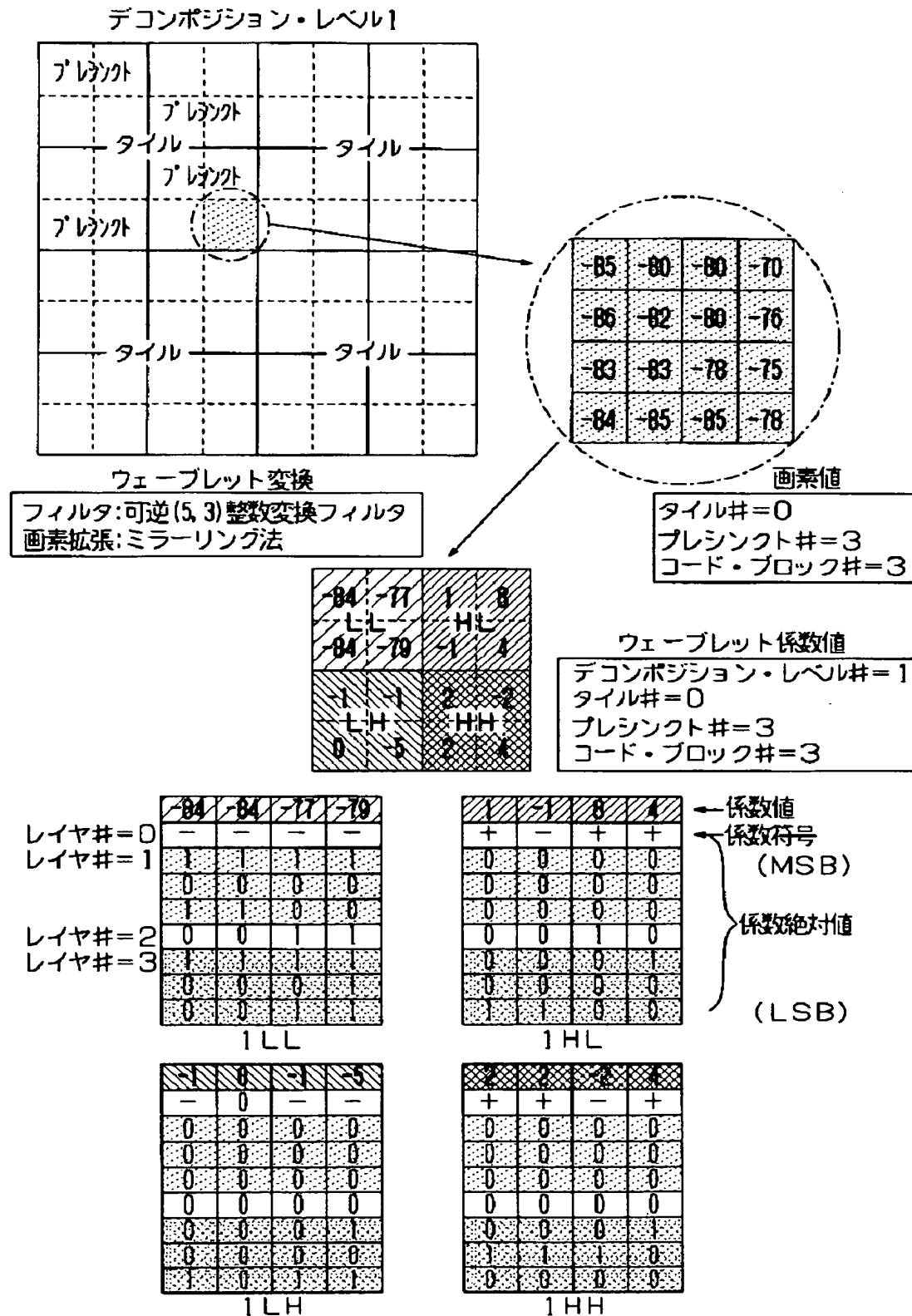
【図 3】



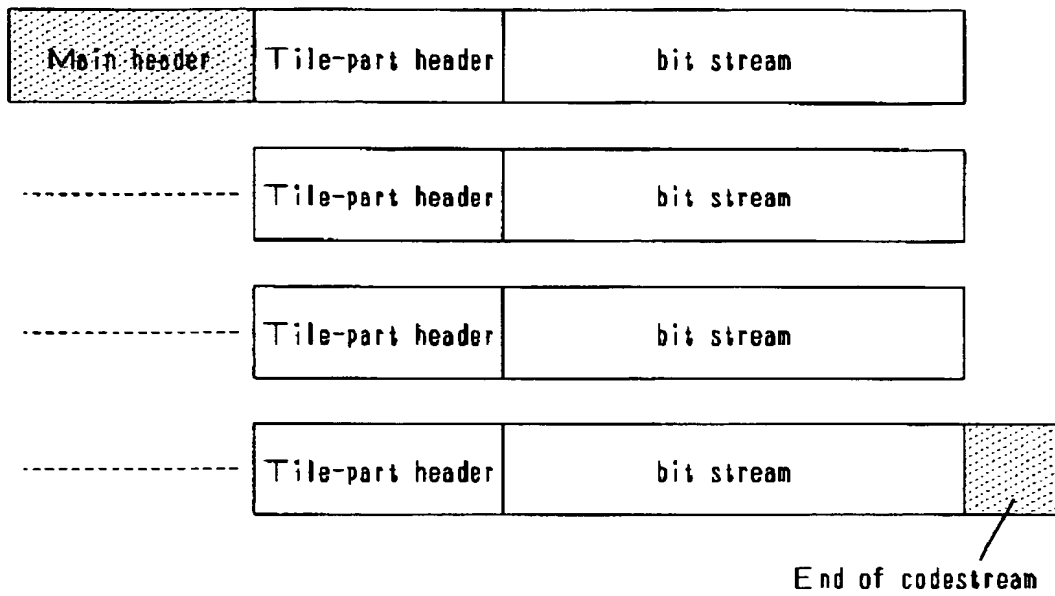
【図 4】



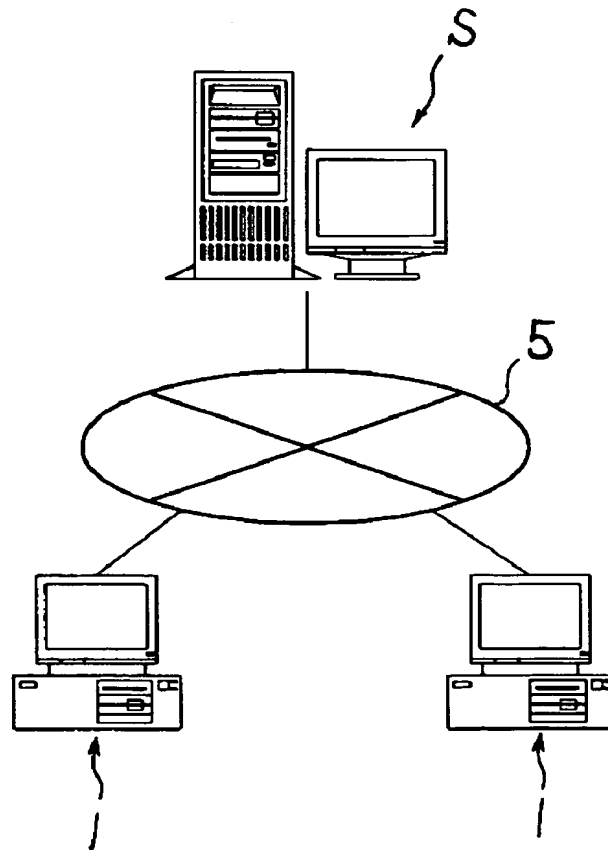
【図 5】



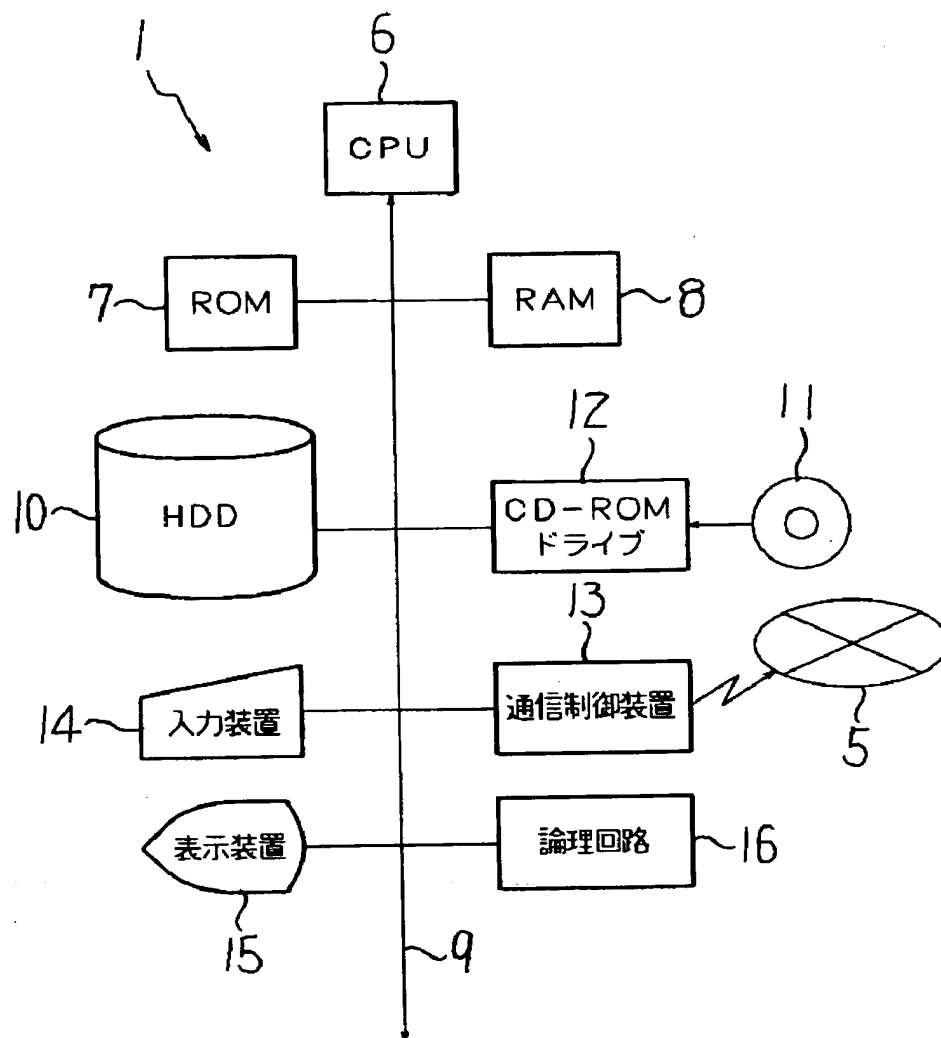
【図 6】



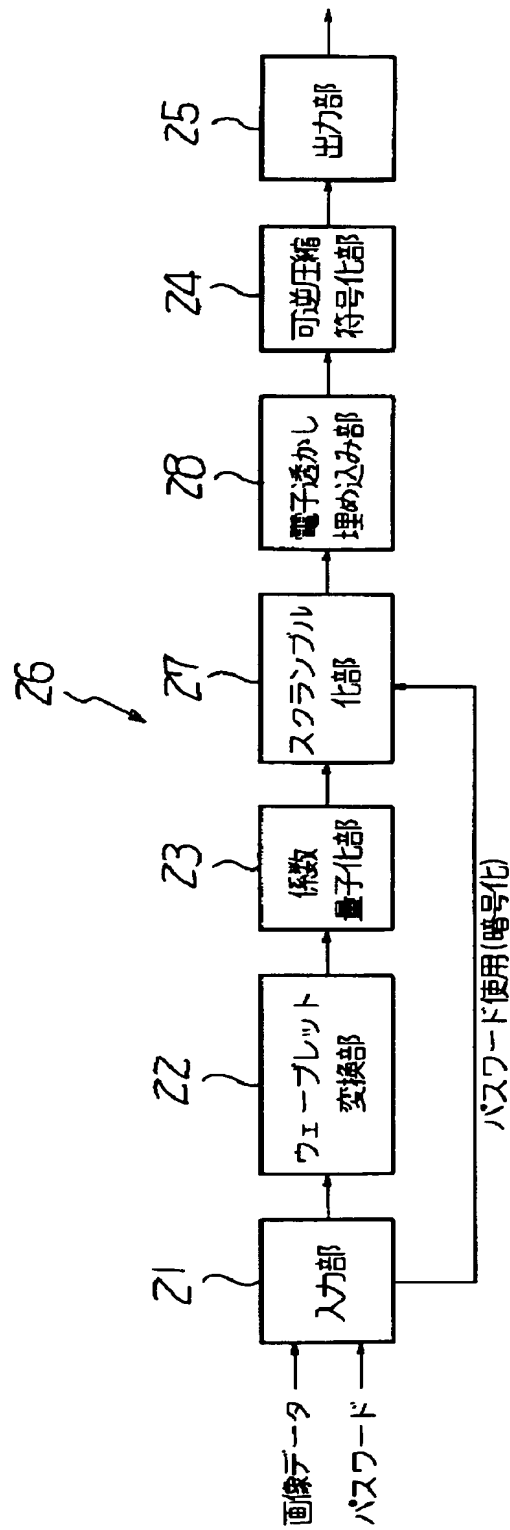
【図 7】



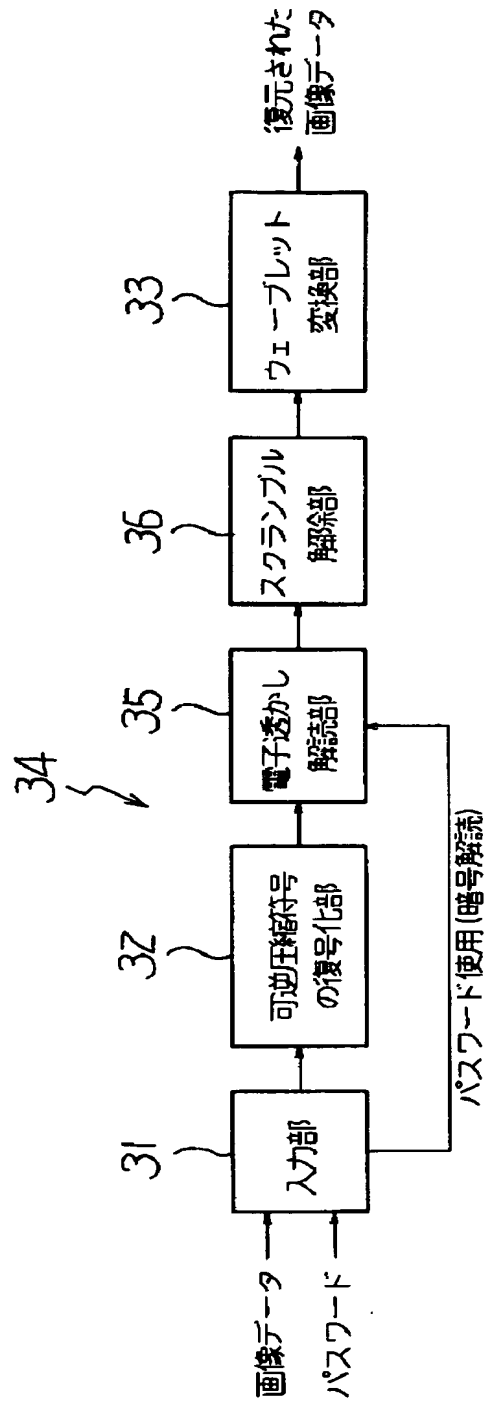
【図 8】



【図 9】

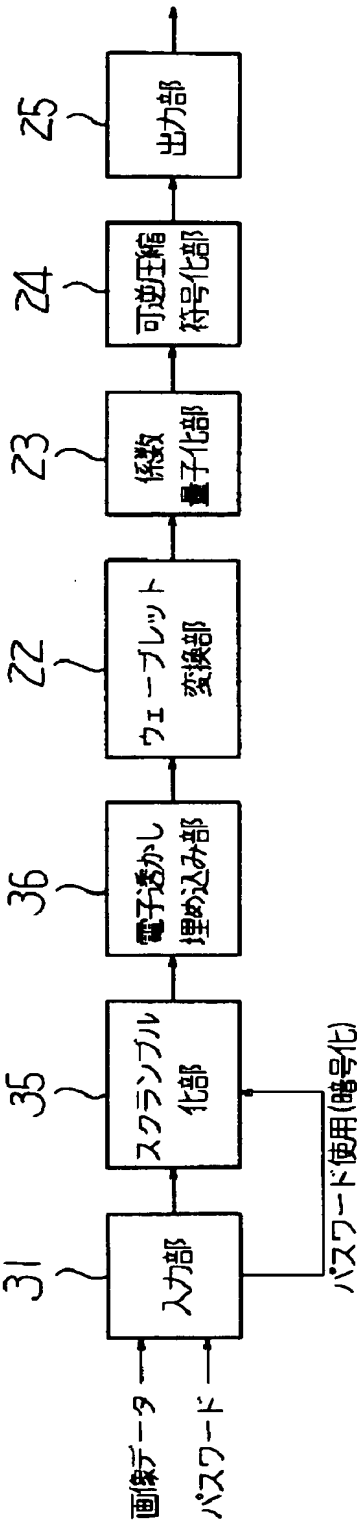


【図 10】





【図 11】



【書類名】 要約書

【要約】

【課題】 スクランブルの影響が残らない復号処理を可能にする。

【解決手段】 入力された画像データを J P E G 2 0 0 0 アルゴリズムの非可逆モードに従い圧縮符号化する圧縮符号化手段 2 6 に対して、この圧縮符号化手段による離散ウェーブレット変換処理後に量子化された離散ウェーブレット変換係数をスクランブル化するスクランブル化手段 2 7 を設けることで、入力された画像データを J P E G 2 0 0 0 アルゴリズムの非可逆モードに従い圧縮符号化する場合であっても、量子化処理の後には可逆的な処理となるので、その直前のデータである離散ウェーブレット変換処理後に量子化された離散ウェーブレット変換係数にスクランブルをかけてもそのスクランブルも可逆的に完全に復号させることで、復号に際しては完全にスクランブルの影響をなくすることが可能となる。

【選択図】 図 9

特願 2003-013591

出 願 人 履 歴 情 報

識別番号

[000006747]

1. 変更年月日

2002年 5月17日

[変更理由]

住所変更

住 所

東京都大田区中馬込1丁目3番6号

氏 名

株式会社リコー